

**Intrusion Prevention Service (IPS) arbeitet mit der Content-Inspection auf Anwendungsebene der WatchGuard XTM-Lösung zusammen und bietet auf diese Weise Echtzeitschutz vor Netzwerkbedrohungen, einschließlich SQL-Einschleusungen, Cross-Site-Scripting und Pufferüberläufen.**

**Warum Sie sich ein IPS-Abonnement anschaffen sollten**

IPS überprüft den Datenverkehr in allen gängigen Protokollen und verwendet aktualisierte Signaturen, um alle Arten von Malware zu erkennen und zu blockieren. Und da IPS in WatchGuard XTM-Appliances integriert ist, steht Ihnen eine einfach zu verwaltende, kosteneffiziente Lösung zur Verfügung, ohne dass Sie zusätzliche Hardware erwerben oder verwalten müssen.

**Drei gute Gründe für Intrusion Prevention Service für Ihre Sicherheitslösung: Cross-Site-Scripting-Angriffe, SQL-Einschleusungen und Pufferüberläufe.**



# Intrusion Prevention Service

Ein integriertes Sicherheits-Abonnement für WatchGuard® XTM-Appliances



## IPS blockiert Netzwerkangriffe

Die Content-Inspection auf Anwendungsebene der WatchGuard XTM-Appliances bietet Schutz vor Netzwerkangriffen, wie Spoofing, Flooding und Denial of Service. Die Intrusion Prevention Service fügt mit einer signaturbasierten Erkennung von Netzwerkangriffen eine weitere Schutzzebene hinzu.

### Identifizierung und Blockierung von Netzwerkangriffen

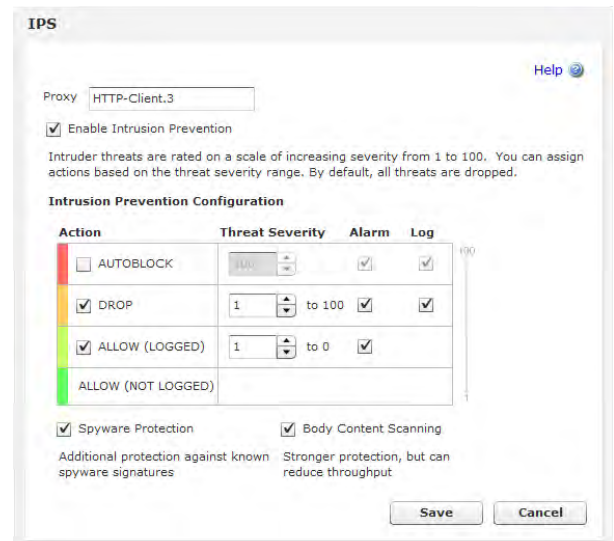
- Umfassender Schutz vor einer breiten Palette bekannter Sicherheitsschwachstellen und Sicherheitslücken in Anwendungen, Datenbanken und Betriebssystemen.
- Mit über 15.000 Signaturen wird eine breite Palette von Bedrohungen abgedeckt, einschließlich SQL-Einschleusungen, Cross-Site-Scripting (XSS), Pufferüberläufen, Denial of Service sowie Remotedateieinschleusungen.
- Die ständig aktualisierte Signaturdatenbank gewährleistet unmittelbaren und umfassenden Schutz. Wenn neue Bedrohungen entstehen, werden neue Signaturen veröffentlicht.
- Überprüfung aller gängigen Protokolle, einschließlich HTTP, HTTPS, FTP, TCP, UDP, DNS, SMTP und POP3, zur Blockierung von Netzwerk-, Anwendungs- und protokollbasierten Angriffen.
- Verhindert, dass Spyware in das Netzwerk gelangt, indem Drive-By-Spyware beim Surfen im Internet blockiert und Spyware identifiziert wird, die versucht, ihren Host zu kontaktieren.

### Detaillierte Steuerung der Reaktion auf Bedrohungen

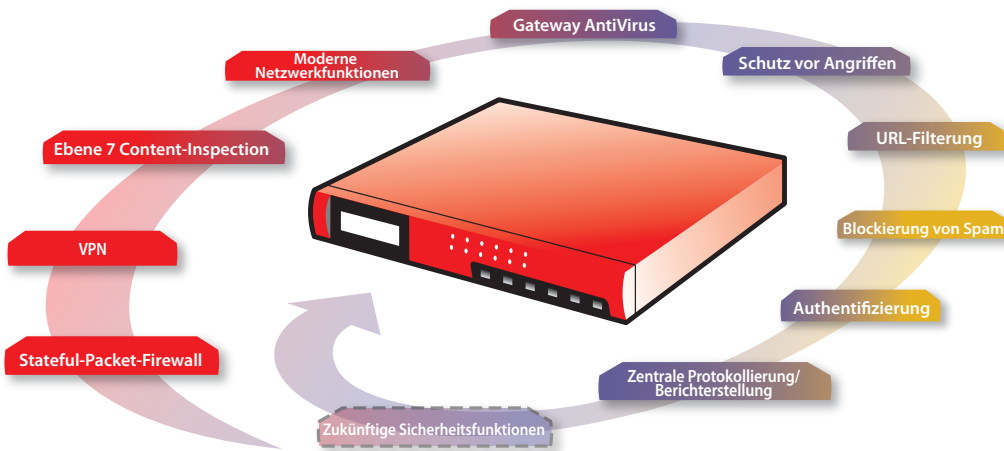
- Zuweisung bestimmter vorzunehmender Maßnahmen in Abhängigkeit von der Stufe der Bedrohung. Jeder Signatur ist ein Schweregrad zugewiesen.
- IP-Adressen, die als Quelle eines Angriffs identifiziert wurden, können automatisch blockiert werden, um zu verhindern, dass bösartiger Datenverkehr erneut in das Netzwerk gelangt.
- Durch die Liste blockierter Seiten wird sichergestellt, dass, sobald eine IP-Adresse als Quelle eines Angriffs identifiziert wurde, zukünftige Angriffe von dieser Adresse dynamisch blockiert werden.
- Bestimmte Signaturen können ausgeschlossen werden. CVE-Namen (Common Vulnerabilities and Exposures) für häufig auftretende Sicherheitslücken und Schwachstellen werden angegeben, falls sie vorhanden sind; dadurch wird die Freigabe von Daten über separate Netzwerksicherheitstools vereinfacht.

### Kosteneffiziente Verhinderung von Angriffen

- Netzwerkweiter Schutz für alle Benutzer, die hinter der WatchGuard XTM-Firewall konfiguriert sind, mit einem einzigen IPS-Abonnement.
- Erwerben Sie IPS im Paket mit unserer Suite leistungsstarker Sicherheits-Abonnements, um noch höhere Kosteneinsparungen zu erzielen, einschließlich WebBlocker, spamBlocker, Gateway AntiVirus und LiveSecurity Service mit technischem Support rund um die Uhr.



## Voll integrierte Sicherheit für umfassenden Schutz



### Komplette Sicherheitslösung

WatchGuard XTM-Appliances können mit leistungsstarken Sicherheits-Abonnements kombiniert werden und bieten auf diese Weise umfassenden Schutz vor Malware. Alle Sicherheitsfunktionen werden von einer intuitiven Konsole aus verwaltet; diese umfasst zentrale Protokollierungs- und Berichterstellungsfunktionen für eine hochaktuelle Ansicht der sicherheitsrelevanten Netzwerkaktivitäten.

Da sich Bedrohungen ständig ändern, wurden WatchGuard XTM-Lösungen so konzipiert, dass problemlos neue Netzwerkschutzfunktionen über Sicherheits-Abonnements hinzugefügt werden können, sodass keine kostspieligen Hardware-Upgrades erforderlich sind.

### Die Verwaltung von Sicherheits-Abonnements ist ganz einfach

Alle Sicherheitsfunktionen in Ihrer WatchGuard XTM-Lösung, einschließlich Intrusion Prevention, können für maximale Effizienz und Benutzerfreundlichkeit von einer einzigen intuitiven Konsole aus verwaltet werden.

- Alle von IPS identifizierte Sicherheitsaktivitäten werden für eine einfache Berichterstellung protokolliert und gespeichert, sodass Sie umgehend entsprechende Vorbeuge- oder Korrekturmaßnahmen vornehmen können.
- IT-Administratoren können ganz flexibel die vorzunehmende Maßnahme definieren, wenn Malware identifiziert wird; auf diese Weise kann das Netzwerk fraglichen Datenverkehr basierend auf Typ, Benutzer/Gruppe und Protokoll zulassen, blockieren, in Quarantäne stellen oder sperren.
- Mit dem Kauf der WatchGuard XTM-Appliance stehen Ihnen alle Verwaltungstools, einschließlich umfangreicher Berichterstellungs- und Überwachungstools, zur Verfügung. Sie müssen keine zusätzliche Hardware oder Software erwerben.

### Weitere WatchGuard-Sicherheits-Abonnements

WatchGuard bietet eine vollständige Suite von Sicherheitsdiensten, mit denen Sie den Schutz in wichtigen Bereichen optimieren können. Neben Intrusion Prevention Service gibt es folgende Abonnements:

- **WebBlocker** Über die URL- und Inhaltsfilterung mit HTTP- und HTTPS-Überprüfung können Sie den Zugriff auf Websites steuern, die unerwünschte Inhalte hosten bzw. Risiken für die Netzwerksicherheit bergen, einschließlich bekannter Spyware- und Phishing-Websites.
- **spamBlocker blockiert** nahezu 100 % aller unerwünschten E-Mails in Echtzeit, bevor diese Ihren internen E-Mail-Server oder -Client erreichen. Auf diese Weise wird Ihr Netzwerk durch eine zusätzliche Ebene vor einem Virenausbruch geschützt. spamBlocker umfasst außerdem eine komplette Spam-Quarantäne.
- **Gateway AntiVirus** bietet Echtzeitschutz vor bekannten Viren, Trojanern, Würmern, Spyware und Rogueware.

### Rundum-Sicherheit im Bundle!

Holen Sie sich mit dem Security Bundle von WatchGuard in einem praktischen Paket alles, was Sie für ein vollständiges Bedrohungsmanagement benötigen, einschließlich Firewall, VPN, Sicherheits-Abonnements und technischem Support.

Jedes Security Bundle umfasst Folgendes:

- Eine WatchGuard XTM-Appliance Ihrer Wahl (8 Series oder 10 Series)
- spamBlocker
- WebBlocker
- Gateway AntiVirus
- Intrusion Prevention Service
- LiveSecurity® Service für technischen Support rund um die Uhr, Hardware-Garantie, Software-Updates und Warnmeldungen

Mit dem Bundle wird vom Einkauf bis hin zur ständigen Sicherheitsverwaltung die Netzwerksicherheit einfacher und effizienter gestaltet. Sie erhalten eine komplette Lösung zu einem hervorragenden Preis, ohne zusätzliche Gebühren, Verträge oder Hardware.

### Sie haben bereits eine Appliance? Holen Sie sich die Security Software Suite\*

Wenn Sie bereits eine WatchGuard XTM-Appliance besitzen, ergänzen Sie diese mit der Security Software Suite, um eine Komplettlösung für die Verwaltung von Bedrohungen zu erhalten. Die Suite umfasst alle oben aufgeführten Sicherheits-Abonnements, einschließlich LiveSecurity für Beratung und Support durch Experten. Ein hervorragendes Angebot, wenn Sie das Paket erwerben und sparen!

\*Security Software Suite umfasst keine Appliance.

Für das Security Bundle und die Software Security Suite sind einjährige, zweijährige und dreijährige Abonnementpakete erhältlich.

Adresse: Max-Planck Str. 4, 85609 Aschheim, Germany • Web: [www.watchguard.de](http://www.watchguard.de) • Telefon: +49 (700) 92229333

In diesem Dokument werden keine ausdrücklichen oder konkludenten Garantien gegeben. Sämtliche hier aufgeführten technischen Daten können jederzeit geändert werden. Informationen zu zukünftigen Produkten, Merkmalen und Funktionen werden zum gegebenen Zeitpunkt zur Verfügung gestellt. © 2009 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard-Logo und LiveSecurity sind Marken oder eingetragene Marken von WatchGuard Technologies, Inc. in den USA und/oder anderen Ländern. Alle anderen Markennamen sind Eigentum ihrer jeweiligen Inhaber. Teilnr. WCC66652\_101609